WIRELESS G PC CARD USER MANUAL

MODEL 505314

INTELLINET
NETWORK SOLUTIONS

INT-505314-UM-0508-01

Thank you for purchasing the INTELLINET NETWORK SOLUTIONS™ Wireless G PC Card, Model 505314.

Compatible with 802.11b and 802.11g wireless access points and routers, this adapter lets you upgrade your wireless network without the need to replace existing equipment. Transfer or receive digital images, videos and MP3 files with link speeds of up to 54 Mbps using proven and reliable Wireless G technology. With the easy-to-follow instructions in this manual, you'll soon be able to enjoy the benefits of these additional features:

- Connects your notebook to a wireless network
- Turbo Mode technology for enhanced wireless throughput
- Supports WEP (64/128 bit), WPA and WPA2 data encryption
- Supports Software AP function (turns your wireless client into a wireless access point)
- Supports WMM (Wi-Fi Multimedia) for increased multimedia data throughput
- Windows 98SE/2000/Me/XP/Vista compatible
- 32-bit Cardbus PC card
- Lifetime Warranty

FCC Certifications

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CAUTION: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference; and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment, and should be installed and operated with a minimum distance of 2.5 cm (1 in.) between the radiator and your body.

SAR (specific absorption rate) compliance has been established in laptop computer configurations with a USB port on the side near the center, as tested in the application for certification, and can be used in laptops with substantially similar physical dimensions, construction and electrical and RF characteristics. Use in other devices, such as PDAs or lap pads, is not authorized. This transmitter is restricted for use with the specific antenna(s) tested in the application for certification. The antenna(s) used for this transmitter must not be co-located or operated in conjunction with any other antenna or transmitter.

R&TTE Compliance Statement

This equipment complies with all the requirements of Directive 1999/5/EC of the European Parliament and the Council of March 9, 1999, on radio equipment and telecommunication terminal equipment (R&TTE) and the mutual recognition of their conformity. The R&TTE directive repeals and replaces Directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) as of April 8, 2000.

EU Countries Intended for Use

The ETSI version of this device is intended for home/office use in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden and the U.K., and is also authorized for use in EFTA member states Iceland, Liechtenstein, Norway and Switzerland. (EU countries not intended for use: none.)

TABLE OF CONTENTS

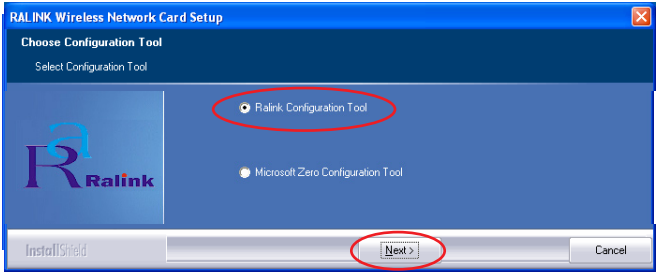
NOTE: Some screen-shot images have been modified to fit the format of this user manual.

INSTALLATION

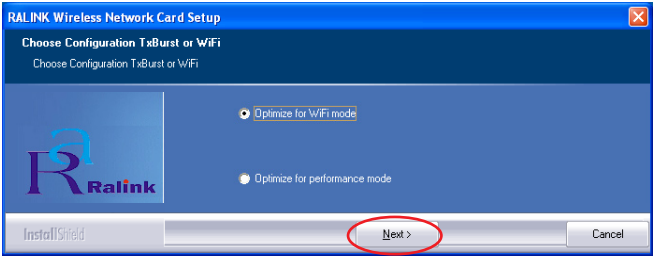
Prior to connecting the Wireless G PC Card (also referred to as an “adapter”):

- Uninstall any previously loaded versions of the driver and utility.
- Install the software program from the CD. ***NOTE:*** The following Windows XP procedure is similar for Windows 98SE/Me/2000/2003/Vista.

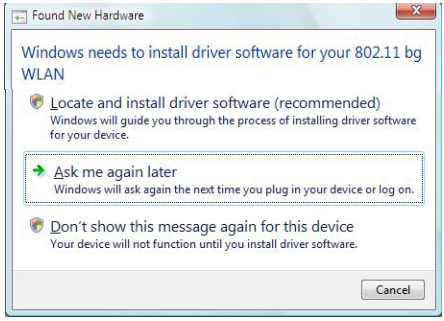
1. Insert the setup CD in the CD-ROM drive and run the setup program.
2. Read the license agreement that displays; click “Yes” to proceed.
3. In Windows XP, a “Microsoft (Windows) Zero Configuration Tool” option displays. It’s recommended that the alternative “Ralink Configuration Tool” option be selected, as it features more functions. Click “Next.”



4. To run the adapter at a higher speed, select “Optimize for performance” to enable the Tx Burst mode. Otherwise, “Optimize for WiFi” sets the adapter to run with a standard wireless network. Click “Next.”



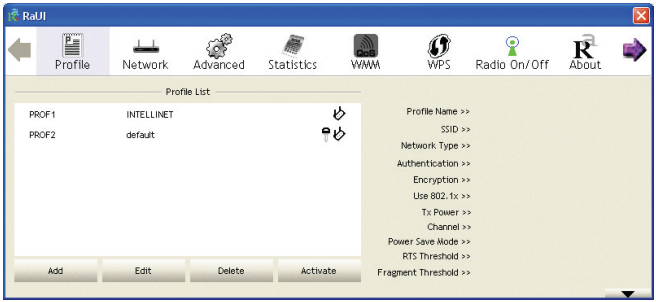
5. Once the software installation begins, a Setup Status screen is followed by a prompt to connect the Wireless G PC Card to your computer. The system automatically detects the card. ***NOTE:*** In Windows Vista, a Found New Hardware screen appears (above) when the card is connected. You can ignore the message, as it disappears once installation is complete.



6. When the Finish screen appears, click "Finish."

CONFIGURATION

The configuration utility — which displays automatically once the card is connected — is a powerful application that helps you configure the card and monitor link status and statistics during the communication process. This card/adapter will auto-connect to the wireless device that has the better signal strength and no wireless security setting.



The configuration utility appears as an icon in the Windows system tray while the adapter is running. You can open it by double-clicking on the icon.

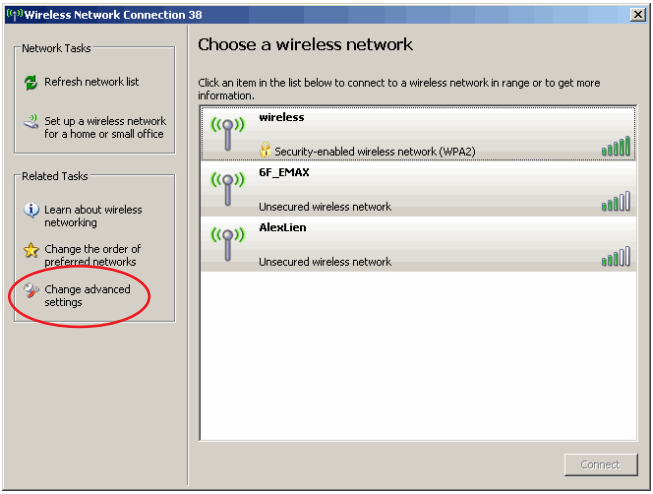
In Windows XP, there is a “Windows Zero Configuration Tool” option for setting up wireless clients. If you prefer to use the configuration utility, there are two ways to switch to it instead of using the Windows tool.

Option 1

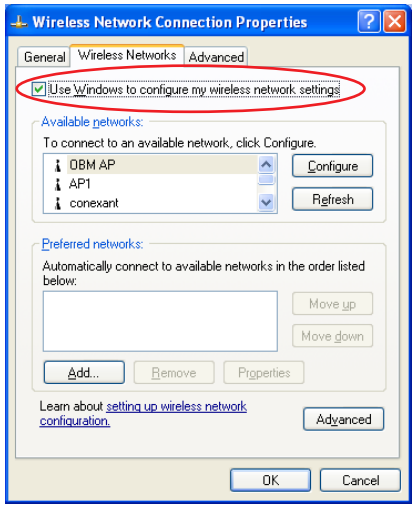
1. Right-click the utility icon in the system tray and select “Use RaConfig as Configuration utility.”

Option 2

1. Right-click the icon on the left side of the system tray and select “View Available Wireless Networks.”
2. Click “Change advanced settings.”

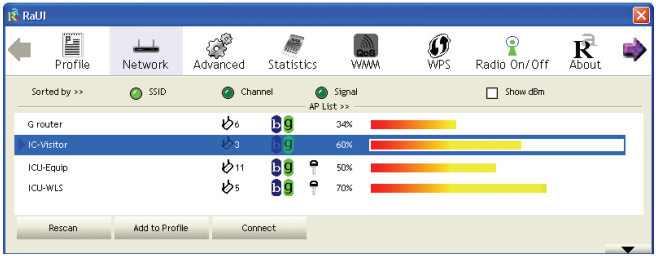


3. Uncheck “Use Windows to configure my wireless network settings” to enable the utility for the adapter. ***NOTE:*** If “Wireless Zero Configuration Tool” is enabled, you can only configure the advanced settings or check the link status and statistics from the configuration utility of the adapter.



NETWORK

When you open the configuration utility, the system scans all the channels to find access points/stations within the accessible range of the adapter and automatically connect to the wireless device with the highest signal strength. On the Network screen, all the networks nearby are listed. You can change the connection to another network or add one of the networks to your own profile list.



Available Networks: This list shows all available wireless networks within the range of the adapter. It also displays network information: SSID, BSSID, Signal Strength, Channel, Encryption, Authentication and Network Type. To connect to a network on the list, double-click the item and the adapter will connect automatically to it.

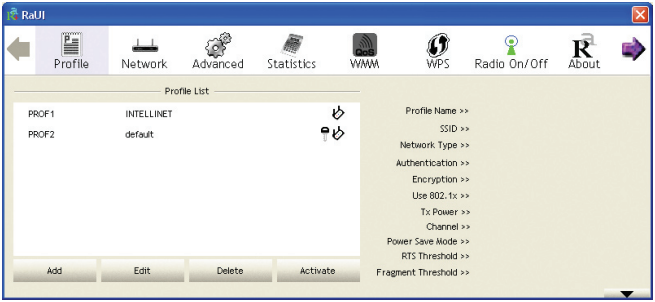
Rescan: Click "Rescan" to collect the new information of all the wireless networks nearby.

Connect: Click "Connect" to connect to the selected network.

Add to Profile: Click to add the selected network to the Profile list.

PROFILE

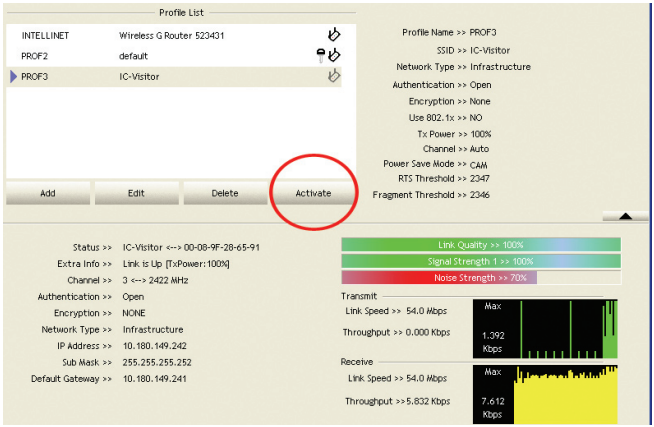
The Profile screen is for managing networks you connect to frequently. You can add, delete, edit and activate a profile on this screen.



Profile List: The Profile List displays all the profiles and their related settings, including Profile Name, SSID, Channel, Authentication, Encryption and Network Type.

Add, Edit, Delete: Click the corresponding button to add, edit or delete the selected profile(s). Clicking "Add" displays the Add Profile screen, which presents 1) Configuration and 2) Authentication and Encryption (Security).

Activate: To display status information about your current wireless connection, select the profile and click "Activate." When a profile is activated, the adapter will be initially connected to it.



Status: This field displays the SSID and MAC ID of the network the adapter is connecting to.

Extra Info: This field displays the link status.

Channel: This field displays the number of the radio channel and the frequency used for the networking.

Link Speed (Mbps): These fields display the transmission (Tx) and the reception (Rx) rates of the network. The maximum transmission rate is 54 Mbps.

Throughput (Kbps): These fields display the speed of data being transmitted (Tx) and received (Rx).

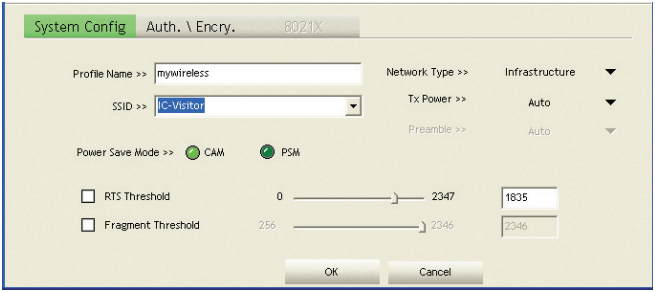
Link Quality: This status bar indicates the quality of the link. The higher the percentage, the better the quality.

dBm: To display the signal strength measured in dBm (decibels in milliwatts), click this box on the Network screen (see Page 9).

Signal Strength: This bar shows the signal strength level. The higher the percentage being shown in the bar, the more radio signal being received by the adapter. This indicator helps to find the proper position of the wireless device for quality network operation.

Noise Strength: This bar displays the noise level in the wireless environment.

Profile Configuration



Profile Name: Define easily recognizable profile names to identify the different networks.

SSID: The SSID (up to 32 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs. If you specify an SSID for the adapter, then only the device with the same SSID can interconnect to the adapter. To add a nearby network to the profile list, pull down the menu to view all the networks that can be selected.

Power Save Mode: The two power-saving functions are available only when Network Type (see below) is set to "Infrastructure."

- **CAM (Constantly Awake Mode):** With this selected, the adapter will remain in an active mode.
- **PSM (Power Save Mode):** Enable the adapter in the power-save mode when it is idle.

Network Type: Select from the drop-down menu.

- **Infrastructure:** This operation mode requires the presence of an 802.11 access point. All communication is done via the AP or router.
- **Ad-Hoc:** Select this mode to connect to another wireless station in the wireless LAN network without using an access point or router.

Tx Power: To lower the transmit power of the adapter to reduce the power used by the system, select a lower percentage from the drop-down menu. ***NOTE:*** A lower power level will result in lower signal strength and reduced coverage range.

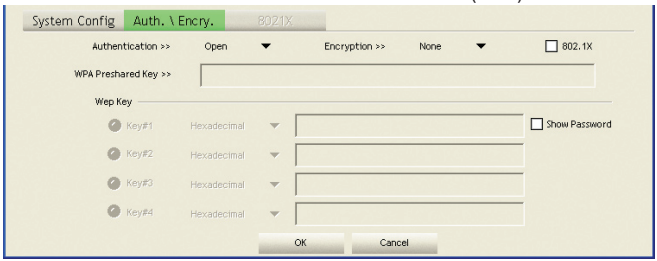
RTS Threshold: This is the minimum packet size required for an RTS (request to send). For packets smaller than this threshold, an RTS is not sent and the packet is transmitted directly to the wireless network. Select a setting within a range of 0 to 2347 bytes. ***NOTE:*** A minor change is recommended.

Fragment Threshold: This value defines the maximum size of packets; any packet size larger than the value will be fragmented. If you've decreased this value and experience high packet-error rates, you can increase it again, but it will likely decrease overall network performance. Select a setting within a range of 256 to 2346 bytes. ***NOTE:*** A minor change is recommended.

Profile Authentication and Encryption (Security)

Authentication Type: This pull-down menu setting has to be consistent with the wireless networks that the adapter is intended to connect.

- **Open:** No authentication is needed within the wireless network.
- **Shared:** Only wireless devices using a shared key (WEP key identified) are allowed to connect to each other.
- **LEAP:** This is a pre-EAP, Cisco-proprietary protocol with many of the features of EAP protocols. Cisco controls the ability of other vendors to implement this protocol, so it should be selected for use only when a limited vendor choice for client, access point and server products is not a concern. When you've set up LEAP authentication, you need to enter the username and password of your computer.
- **WPA:** WPA provides a scheme of mutual authentication using either IEEE 802.1x/Extensible Authentication Protocol (EAP) authentication



or pre-shared key (PSK) technology. It provides a high level of assurance to enterprises, small businesses and home users that data will remain protected and that only authorized users may access their networks. For enterprises that have already deployed IEEE 802.1x authentication, WPA offers the advantage of leveraging existing authentication databases and infrastructure.

- **WPA-PSK:** This is a special mode designed for home and small business users who do not have access to network authentication servers. In this mode, known as Pre-Shared Key, you manually enter the starting password in your access point or gateway, as well as in each wireless station in the network. WPA-PSK takes over automatically from that point, keeping unauthorized users who don't have the matching password from joining the network, while encrypting the data traveling between authorized devices.
- **WPA2:** Like WPA, WPA2 supports IEEE 802.1x/EAP authentication, or PSK, technology. It also includes a new advanced encryption mechanism using the Advanced Encryption Standard (AES). AES is required for corporate or government users. The difference between WPA and WPA2 is that WPA2 provides data encryption via AES. In contrast, WPA uses the Temporal Key Integrity Protocol (TKIP).
- **WPA2-PSK:** This is also for home and small business use. The difference between WPA-PSK and WPA2-PSK is that WPA2-PSK provides data encryption via the AES. In contrast, WPA-PSK uses the Temporal Key Integrity Protocol (TKIP).
- **WPA-NONE:** This is defined for Ad Hoc mode and behaves like WPA-PSK (WPA-PSK is only defined for Infrastructure mode). The user manually enters the Pre-Shared Key in each wireless station in the network, and WPA-NONE controls unauthorized users who don't have the matching Pre-Shared Key from joining the network. It also encrypts the data traveling between authorized devices.

802.1x Setting: When Authentication Type is set to "Open," "Shared," "WPA" or "WPA2," you can also enable IEEE 802.1x Setting to use the authentication server or certification server to authenticate client users.

NOTE: See the two separate 802.1x Setting sections below for details.

Encryption: Select from the drop-down menu.

- **None:** Disables the encryption mode.

- **WEP:** Enables the WEP Data Encryption. When the item is selected, you need to continue setting the WEP Encryption keys.
- **TKIP:** The Temporal Key Integrity Protocol changes the temporal key every 10,000 packets (a kind of message transmitted over a network.) This ensures much greater security than the standard WEP security.
- **AES:** AES has been developed to ensure the highest degree of security and authenticity for digital information. It's the most advanced solution defined by IEEE 802.11i for security in the wireless network. ***NOTE:*** All devices in the network should use the same encryption method to ensure the security of communications.

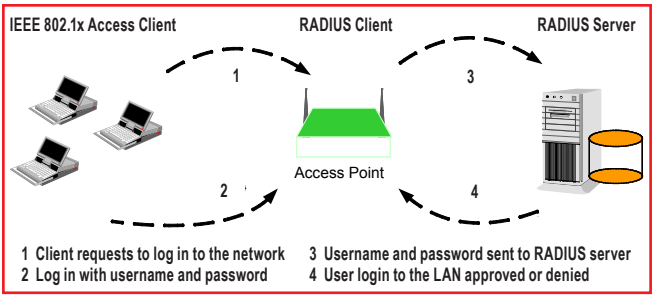
WPA Pre-Shared Key: The WPA-PSK key can be 8 to 64 characters in length and can be letters or numbers. This same key must be used on all the wireless stations in the network.

WEP Key (Key#1–4): WEP keys are used to encrypt data transmitted in the wireless network. There are two types of key length: 64-bit and 128-bit. Assign a default encryption key (Key#1 to Key#4) by clicking on the corresponding radio button. To fill in each text field:

- **64-bit:** Input 10-digit hex values (in the A-F, a-f and 0-9 range) or 5-digit ASCII characters (a-z and 0-9) as the encryption keys. For example: "0123456aef" or "test1."
- **128-bit:** Input 26-digit hex values (in the A-F, a-f and 0-9 range) or 13-digit ASCII characters ("a-z" and "0-9") as the encryption keys. For example: "01234567890123456789abcdef" or "administrator."

The IEEE 802.1X specification describes a protocol that can be used for authenticating both clients (802.1x Setting/Certification below) and servers (802.1x Setting/CA Server below) on a network. The authentication algorithms and methods are those provided by the Extensible Authentication Protocol (EAP), a method of authentication that has been in use for a number of years on networks that provide Point-to-Point Protocol (PPP) support (as many Internet service providers and enterprises do). EAP runs before network layer protocols transmit data over the link.

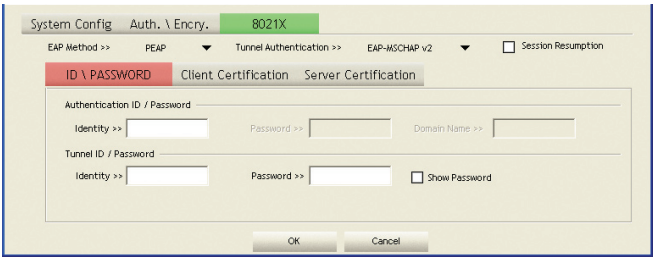
When an AP acting as an authenticator detects a wireless station on the LAN, it sends an EAP request for the user's identity to the device. In turn, the device responds with its identity, and the AP relays this identity to an authentication server (typically an external RADIUS server).



802.1x Setting/Certification

EAP Method: The EAP authentication protocols supported by this adapter require that settings be consistent with the wireless access points or routers that the adapter is intended to connect.

- **PEAP & TTLS:** These protocols are similar and easier to use than TLS (below) in that they specify a stand-alone authentication protocol to be used within an encrypted tunnel. TTLS supports any protocol within its tunnel, including CHAP, MS-CHAP, MS-CHAPv2, PAP and EAP-MD5. PEAP specifies that an EAP-compliant authentication protocol be used; this adapter supports EAP-MSCHAP v2, EAP-TLS/ Smart Card and Generic Token Card. The client certificate is optional.
- **TLS/Smart Card:** This is the most secure of the EAP protocols, but isn't easy to use: It requires that digital certificates be exchanged in



the authentication phase. The server presents a certificate to the client and, after validating the server's certificate, the client presents a client certificate to the server for validation.

Session Resumption: Click/check the box to activate or de-activate.

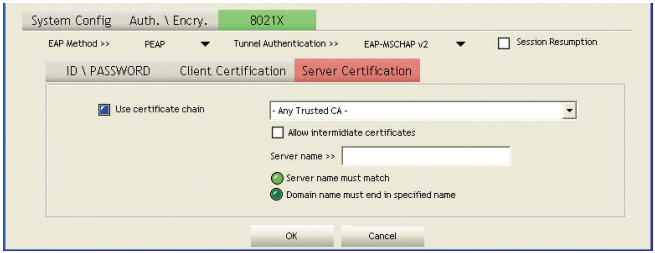
ID/Password: Enter the password as the identity for the server.

Client Certification: A client certificate is required for TLS, but is optional for TTLS and PEAP. This forces a client certificate to be selected from the appropriate Windows Certificate Store and made available to the RADIUS server for certification.

Tunneled Authentication/Protocol: When the authentication type is PEAP or TTLS, select a protocol for building the encrypted tunnel.

Tunnel Authentication: Select one of three options from the drop-down menu: "EAP-MSCHAPv2," "EAP-TLS/Smart card" or "Generic Token Card."

802.1x Setting/CA Server



Use certificate chain: When the Extensible Authentication Protocol (EAP) authentication type — such as TLS, TTLS or PEAP — is selected and requires certification to tell the client what credentials to accept from the authentication server in order to verify the server, you need to enable this function. Choose the preferred server from the drop-down menu to issue the certificate. If "Any Trusted CA" is selected, any CA (certification authority) on the list (which is provided by the Microsoft Certificate Store) is permitted.

Allow intermediate certificates: A server designates an issuer as a trusted root authority by placing the issuer's self-signed certificate,

which contains the issuer's public key, into the trusted root certification authority certificate store of the host computer. Intermediate or subordinate certification authorities are trusted only if they have a valid certification path from a trusted root certification authority.

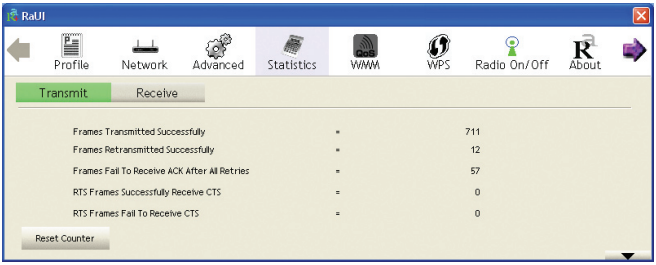
Server Name: Enter the authentication server name.

Server name must match exactly: When selected, the server name must exactly match the server name found on the certificate.

Domain name must end in specified name: When this is selected, the server name field identifies a domain. The certificate must use a server name belonging to this domain or one of its sub-domains (e.g., zeelans.com, where the server is blueberry.zeelans.com), but it may be any name used in the certificate name field.

STATISTICS

This screen enables you to view/compare the transmit and receive statistical information of the connection. To reset the counters, click "Reset Counter."

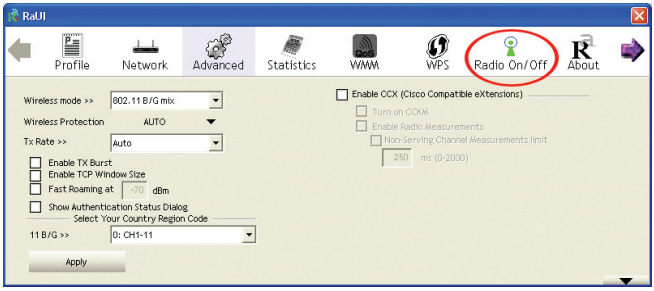


ADVANCED

This screen enables you to configure more advanced settings, such as the wireless mode and the protection mode.

Wireless Mode: Select from the drop-down menu.

- **802.11 B/G mix:** If you have a mix of 802.11b and 802.11g wireless stations in your network, it is recommended that the adapter be set



to this mode. This mode is also the default setting.

- **802.11 B only:** Though the adapter is compatible with both 802.11g and 802.11b wireless stations, if there are only 802.11b wireless stations in the network, you can set the adapter to this mode.

Ad Hoc Wireless Mode: When the adapter is set in Ad Hoc (Peer to Peer) mode, you can designate the wireless connection mode for the Ad Hoc network.

- **Only B:** Though the adapter is compatible with both 802.11g and 802.11b wireless stations, if there are only 802.11b wireless stations in the network, you can set the adapter to this mode.
- **B/G Mixed:** If you have a mix of 802.11b and 802.11g wireless stations in your network, it is recommended that the adapter be set to this mode. This mode is also the default setting.
- **Only G:** Though the adapter is compatible with both 802.11g and 802.11b wireless stations, if there are only 802.11g wireless stations in the network, you can set the adapter to this mode.

Wireless Protection: If you have a mix of 802.11b and 802.11g wireless stations in the network, it's recommended that you enable the protection mechanism, which can decrease the rate of data collisions between 802.11b and 802.11g wireless stations. When the protection mode is enabled, the throughput of the adapter will be a little lower.

- **Auto:** Depending on the status of the network, this automatically disables/enables the protection mode.
- **On:** Always enables the protection mode.
- **Off:** Always disables the protection mode.

Tx Rate: There are several options in the drop-down menu: “Auto” and a range of speeds from “1 Mbps” to “54 Mbps.” When “Auto” is selected, the device automatically chooses the most suitable transmission rate. The higher the data rate designated in the network, the shorter the distance allowed between the adapter and the wireless stations.

When the wireless mode is “802.11 B Only,” the maximum data rate is 11 Mbps (11b), making only “Auto,” “1 Mbps,” “2 Mbps,” “5.5 Mbps” and “11 Mbps” available as options.

Enable Tx Burst: This enables the adapter to deliver better throughput in the same period and environment.

Enable TCP Window Size: The TCP window is the amount of data a sender can deliver on a particular connection before it gets an acknowledgment back from the receiver that it has gotten some of it. When the router or AP the adapter is connecting to has set up the TCP window, you can enable the parameter to meet the data size for the router or AP connection. The larger the TCP window, the better the performance.

Fast Roaming at [-70] dBm: To fast roam to a nearby network without interrupting the wireless connection (such as a multimedia application or a voice call), you can set this parameter. The adapter will fast roam when the receive sensitivity (signal strength) is below the value entered.

Show Authentication Status Dialog: Select to display.

Select Your Country Region Code: Channel availability varies from country to country; for example, USA (FCC) channels are 1-11, while Europe (ETSI) channels are 1-13.

Enable CCX: Cisco Compatible Extensions, for radio monitoring and fast roaming.

Turn on CCKM: During normal operation, LEAP-enabled client devices mutually authenticate with a new AP by performing a complete LEAP authentication, including communication with the main RADIUS server.

When a wireless LAN is configured for fast re-association, however, LEAP-enabled client devices roam from one access point to another without involving the main server. Using Cisco Centralized Key Management (CCKM), an access point configured to provide wireless domain services (WDS) takes the place of the RADIUS server and

authenticates the client so quickly that there is no perceptible delay in voice or other time-sensitive applications.

Enable Radio Measurement: When this parameter is enabled, the Cisco AP can run the radio monitoring through the associated CCX-compliant clients to continuously monitor the WLAN radio environment and discover any new APs that are transmitting beacons.

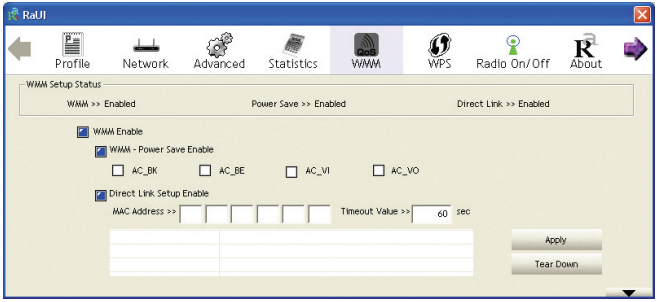
Non-Serving Channel Measurements: The Cisco access point can perform monitoring measurements through the CCX-compliant clients on the non-serving channels when this parameter is enabled.

Limit [xxx] milliseconds (0-2000): This setting limits the channel measurement time. The default value is 250 milliseconds.

Turn off RF: Click to turn off the radio of the adapter; click again to turn it back on.

WMM

This screen enables you to configure WMM (Wi-Fi Multimedia) and other QoS settings, such as Power Save and Direct Link Setup.



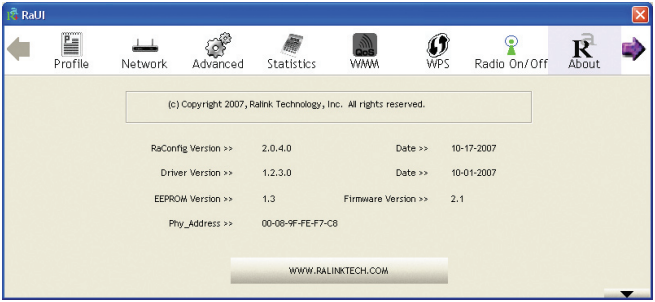
WMM Enable: Click the check box (then click "Apply") to enable the WMM function, which then lets you configure the WMM Power Save and Direct Link Setup functions.

- **WMM – Power Save Enable:** Click the check box to enable, then click "Setting" to further configure the function as "AC_BK," "AC_BE," "AC_VI" or "AC_VO."

- **Direct Link Setup Enable:** Click the check box to enable, then click "Apply" to further configure the function (all within the Direct Link panel).
  - **MAC Address:** Specify the MAC address of the client adapter you want to direct link to and click "Apply" to add to the DLS Status table (below).
  - **Timeout Value:** Specify the timeout value for the direct link being set up.

ABOUT

On this screen, you can click the hyperlink for information on the wireless chipset manufacturer. Basic information about the utility (driver, EEPROM version, etc.) also displays, as do various addresses for quick reference.

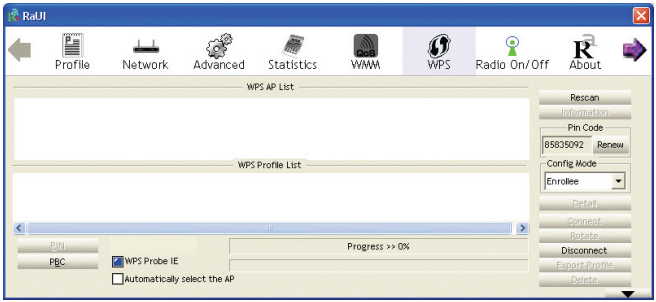


NOTE: This adapter features Turbo Mode, which delivers a higher throughput than IEEE 802.11g standard (up to 54 Mbps) by compressing data and decreasing the wait time for sending data to routers or access points. Turbo Mode is enabled automatically without any configuration.

WPS CONFIGURATION

The adapter supports WPS (Wi-Fi Protected Setup), allowing connection to wireless APs without complicated procedures. Two WPS configuration methods are available: PBC (push-button configuration) and PIN.

WPS AP List: Wireless access points offering WPS service are shown



in this list. If the list is empty, that means that no WPS-enabled AP is in the range.

WPS Probe IE: The Wireless Provisioning Services Information Element (WPS IE) makes it easier to connect to public Wi-Fi networks you've not previously connected to. Your computer must have the WPS IE update for Windows XP SP2 installed in order to use the function.

Automatically select the AP: Select to activate.

Rescan: Click to scan for WPS-enabled APs (perform a site survey).

Information: Select a found WPS-enabled access point, then click "Information" to display that AP's details in a pop-up window.

PIN Code: The WPS PIN Code of this network adapter is required for connection.

SSID (lower panel): The service set identifier of the connected WPS-enabled access point.

MAC Address: The MAC address of connected WPS-enabled AP.

Authentication (lower panel): The authentication type of connected WPS-enabled access point.

Encryption (lower panel): The encryption type of the connected WPS-enabled access point

Detail: Click to show details of a selected WPS-enabled access point.

Connect: Click to connect to a WPS-enabled access point on the list.

Rotate: Click to connect to next WPS-enabled access point on the list.

Disconnect: Click to disconnect from a connected WPS-enabled access point. If there are other wireless access points in the profile, the last

one will be connected; if there's nothing in the profile, the adapter will connect to any unsecured wireless AP nearby.

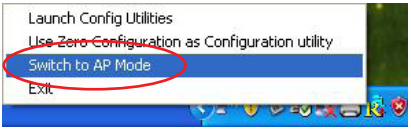
Delete: Delete the WPS-enabled access point from the list.

PIN: To use the PIN-type WPS configuration option, enter the PIN code and then click "PIN."

PBC: To use the PBC-type WPS configuration option, put the WPS-enabled access point in WPS – PBC mode, then click "PBC."

SoftAP

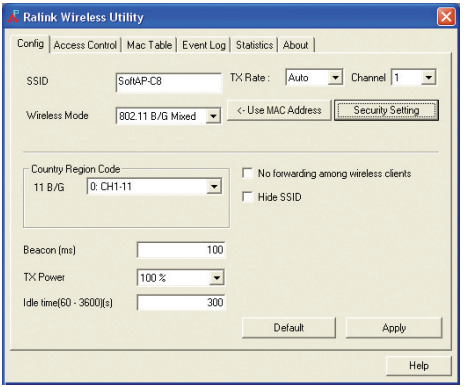
This adapter can run as a wireless access point (AP). Right-click the configuration utility icon on the Windows system tray and select "Switch to AP Mode" to activate the SoftAP function.



CONFIGURATION

This screen enables you to configure the AP connection setting, the Country Region Code and other advanced functions.

SSID: The SSID (up to 32 printable ASCII characters) is the unique name identified in a wireless LAN. The ID prevents the unintentional merging of two co-located WLANs. The default SSID of the AP is "SoftAP-X." ("X" is the last number



of this adapter's MAC address). Wireless adapters connected to the access point should be set up with the same SSID as the AP.

Tx Rate: There are several options in the drop-down menu: "Auto" and a range of speeds from "1 Mbps" to "54 Mbps." When "Auto" is selected, the device automatically chooses the most suitable transmission rate. The higher the data rate designated in the network, the shorter the distance allowed between the adapter and the wireless stations. When the wireless mode is "802.11 B Only," the maximum data rate is 11 Mbps (11b), making only "Auto," "1 Mbps," "2 Mbps," "5.5 Mbps" and "11 Mbps" available as options.

Channel: Select the number of the radio channel used by the access point. Any wireless adapters connected to the AP should be set up with the same channel.

Wireless Mode: Selects the wireless mode supported by the AP.

- **802.11 B/G Mixed:** The AP works in 11b+g mixed mode.
- **802.11 B Only:** The AP works in 11b mode.
- **802.11 G Only:** The AP works in 11g mode.

Use MAC Address: Click to create a unique SSID based on the adapter's MAC address.

Security Setting: Click to further configure WLAN authentication and security settings. (See the separate Security Setting section below.)

Country Region Code: Channel availability varies from country to country; e.g., USA (FCC) channels are 1-11, while Europe's (ETSI) are 1-13.

Beacon (ms): Define the time between beacons (default is 100 ms.)

Tx Power: To lower the transmit power of the AP to reduce the power used by the system, select a lower percentage from the drop-down menu. ***NOTE:*** A lower power level will result in lower signal strength and reduced coverage range.

No forwarding among wireless clients: Enable to prevent wireless clients connected to this AP from sharing information with each other.

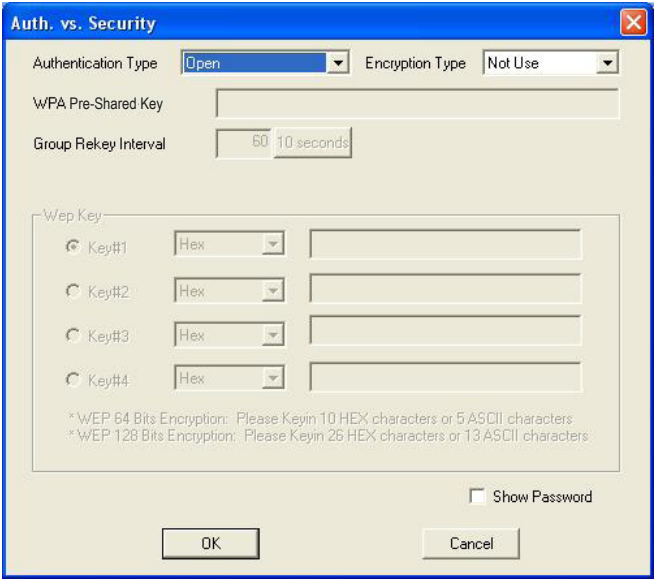
Hide SSID: When this box is checked, the AP will not appear in the site survey list of any wireless clients, meaning only the wireless clients set with the same SSID can connect to the AP. This prevents the AP being connected to by unauthorized users.

Default: Click to use the default value.

Apply: Click to apply the setting change(s).

SECURITY SETTING

This screen — accessed by clicking “Security Setting” on the previous SoftAP Configuration screen — lets you to configure the authentication mode and encryption algorithm used within the AP.



Authentication Type: Four types of authentication mode are supported and presented in the drop-down menu.

- **Open:** No authentication is needed within the wireless network.
- **WPA-PSK:** This is a special mode designed for home and small business users who do not have access to network authentication servers. In this mode, known as Pre-Shared Key, you manually enter the starting password in your access point or gateway, as well as in each wireless station in the network. WPA-PSK automatically takes over from that point, keeping unauthorized users who don’t

have the matching password from joining the network, while encrypting the data traveling between authorized devices.

- **WPA2-PSK:** This is also for home and small business use.
- **WPA-PSK/WPA2-PSK:** When selecting this mode, the AP supports both WPA-PSK and WPA2-PSK.

Encryption Type: Five options are available in the drop-down menu.

- **Not Use:** Disables the encryption mode.
- **WEP:** Enables WEP Data Encryption. When the item is selected, continue setting the WEP Key.
- **TKIP:** The Temporal Key Integrity Protocol changes the temporal key every 10,000 packets (a kind of message transmitted over a network.) This ensures much greater security than standard WEP security.
- **AES:** Advanced Encryption Standard was developed to provide the highest degree of security and authenticity for digital information. It's the most advanced solution defined by IEEE 802.11i for security in a wireless network.
- **BOTH:** In this mode, the AP supports both TKIP and AES.

WPA Pre-Shared Key: The WPA-PSK key can be 8 to 64 characters in length and can be letters or numbers. This same key must be used on all the wireless stations in the network.

Group Rekey Interval: This function is available when using WPA-PSK and WPA2-PSK encryption algorithms.

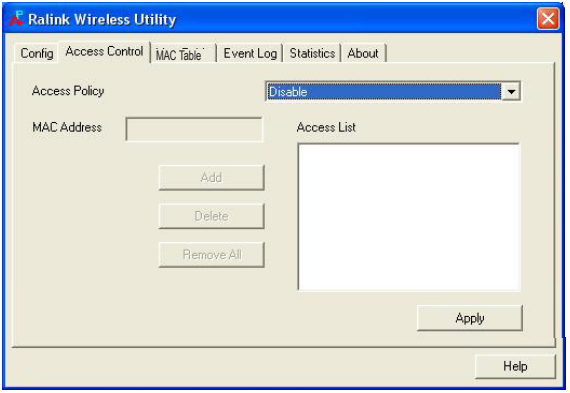
WEP Key (Key#1–4): WEP keys are used to encrypt data transmitted in the wireless network. There are two types of key length: 64-bit and 128-bit. Assign a default encryption key (Key#1 to Key#4) by clicking on the corresponding radio button. To fill in each text field:

- **64-bit:** Input 10-digit hex values (in the A-F, a-f and 0-9 range) or 5-digit ASCII characters (a-z and 0-9) as the encryption keys. For example: "0123456aef" or "test1."
- **128-bit:** Input 26-digit hex values (in the A-F, a-f and 0-9 range) or 13-digit ASCII characters ("a-z" and "0-9") as the encryption keys. For example: "01234567890123456789abcdef" or "administrator."

Show Password: The password will be displayed in clear text instead of with asterisks.

ACCESS CONTROL

This screen lets you configure the access control policy used within the access point.



Access Policy: Select from the drop-down menu.

- **Disable:** Disables the MAC address filtering function.
- **Allow All:** Only wireless adapters with a MAC address on the access list can connect to the AP.
- **Reject All:** Wireless adapters with a MAC address on the access list will be prevented from connecting to the AP.

MAC Address: This is the unique 12-digit hexadecimal identification for hardware devices in the network.

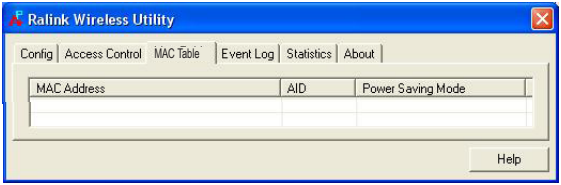
Access List: Displays all the MAC address that have been added.

- **Add:** Add the MAC address to the access list.
- **Delete:** Delete the selected MAC address from the access list.
- **Remove All:** Remove all MAC addresses from the access list.

Apply: Click to apply the setting change(s).

MAC TABLE

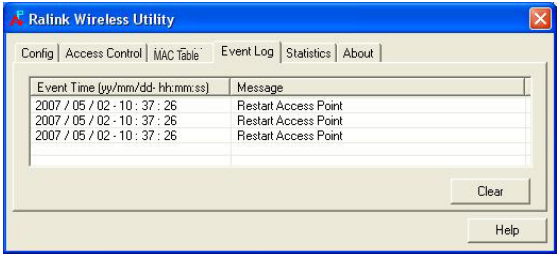
This screen displays details of the wireless adapters connected to the AP.



MAC Address: The addresses of wireless adapters connected to the AP.
AID: The Association ID of the current connection.
Power Saving Mode: The supporting status of the power saving mode of the connected wireless adapter.

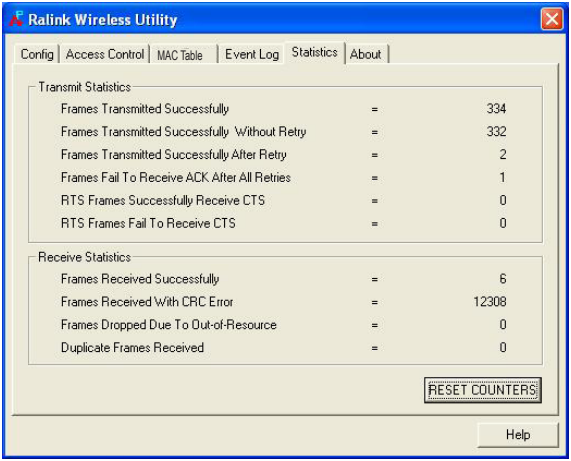
EVENT LOG

This screen displays event times and messages. Click “Clear” to remove displayed information.



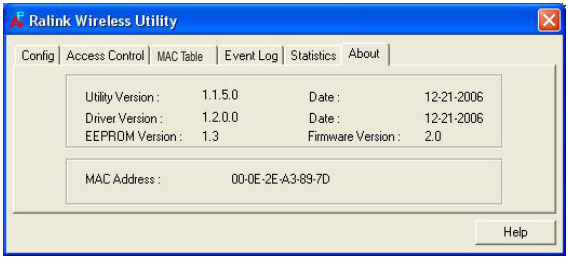
STATISTICS

This screen displays the transmit and receive statistical information of the AP. Click “Reset Counters” to clear the data.



ABOUT

This screen displays basic information about the utility, including the MAC address.



SPECIFICATIONS

General

- Standards:
  - IEEE 802.11b (11 Mbps Wireless LAN)
  - IEEE 802.11g (54 Mbps Wireless LAN)
  - IEEE 802.1X (RADIUS Authentication)
- Bus type: 32-bit PC card
- Chipset: Ralink RT256x
- Frequency band: 2.4000 – 2.4835 GHz (Industrial Scientific Medical Band)
- Modulation technologies:
  - 802.11b: Direct Sequence Spread Spectrum (DSSS): DBPSK, DQPSK, CCK
  - 802.11g: Orthogonal Frequency Division Multiplexing (OFDM): BPSK, QPSK, 16QAM, 64QAM
- Security:
  - 64/128-bit WEP data encryption
  - WPA and WPA2
  - IEEE 802.1X RADIUS Authentication
  - Cisco CCX
- Transmit power: 54 Mbps OFDM, 15 dBm +/- 1 dBm; 11 Mbps CCK, 18 dBm +/- 1 dBm
- Maximum coverage distance: 100 m / 328 ft. (indoor), 300 m / 980 ft. (outdoor)
- Certification: FCC Class B, CE Mark

LEDs

- Link; TX/RX

Environmental

- Weight: 0.18 kg (0.4 lbs.)
- Operating temperature: 0 – 40°C (32 – 104°F)
- Operating humidity: 10 – 95% RH, non-condensing
- Storage temperature: 0 – 70°C (0 – 158°F)

System Requirements

- Notebook with Pentium 300 MHz-compatible processor or higher
- Windows 98SE/Me/2000/XP/2003/Vista, Linux and MacOS X
- WPA2 encryption requires Windows 2000/XP/2003/Vista
- Available 32-bit PC card slot

Package Contents

- Wireless G PC Card
- Setup CD and user manual

BRINGING NETWORKS TO LIFE

INTELLINET NETWORK SOLUTIONS™ offers a complete line of active and passive networking products.
Ask your local computer dealer for more information or visit

www.intellinet-network.com.